



# UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/354,080	07/15/1999	MASSIMO BALESTRI	21197	4578
22852	7590	05/31/2007	EXAMINER	
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413			KLIMACH, PAULA W	
ART UNIT		PAPER NUMBER		
2135				
MAIL DATE		DELIVERY MODE		
05/31/2007		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/354,080	BALESTRI ET AL.
	Examiner Paula W. Klimach	Art Unit 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 09 February 2007.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-15 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-15 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) All    b) Some \* c) None of:
    1. Certified copies of the priority documents have been received.
    2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |                                                                                      |                                                                   |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date: _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date: _____                                                         | 6) <input type="checkbox"/> Other: _____                          |

## DETAILED ACTION

### *Continued Examination Under 37 CFR 1.114*

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/20/07 has been entered.

### *Response to Arguments*

Applicant's arguments filed 03/20/07 have been fully considered. The newly cited reference, Davis, is used to overcome the deficiencies of Wasilewski that are created by the newly added limitation.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. **Claims 1-3, 5-6, 8-10, and 12-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al (6,157,719) and further in view of Davis (6,058,478).

*In reference to claims 1 and 8,* Wasilewski discloses a method for the controlled delivery of digital services to a user, wherein said services are identified by respective stream of encoded

digital data emitted by said plurality providers (column 4 lines 20-23) and the user is provided with a receiver to receive said digital data streams from said plurality providers (Fig. 1), the receiver being selectively enabled to make use of determined services of a given provider (column 4 lines 41-50). The system includes a single removable user unit to be associated to said receiver for enabling the use of respective determined services of the provider (Fig. 12 in combination with column 21 lines 15-27). An identifying code is incorporated into the digital data stream for the user to enable to receive said determined services (column 4 line 64 to column 5 line 13). The single removable user unit is associated to a processing function capable of security functions by exploiting said identifying code to enable the receiver of the user to make use of said determined services (column 5 lines 23-27).

Wasilewski does not expressly disclose incorporating into the digital data streams respective enabling algorithms to be selectively loaded into the smart card of Wasilewski.

Davis discloses a cryptographic device being remotely modified only by proper authorization (abstract). Davis further discloses selectively loading said enabling algorithm into the user unit of each of the selective users (column 8 lines 15-20) based on the respective identifying codes, upgrade signature (column 9 lines 30-51). The enabling algorithm is generated by the provider and specific to the provider (column 9 lines 1-30).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the servers of Wasilewski to create the upgrade or modify cryptographic algorithm by an authorized entity as in Davis. One of ordinary skill in the art would have been motivated to do this because it may be possible to ease export restrictions and allow regional

Art Unit: 2135

licenses for such modifiable cryptographic devices which would greatly reduce the costs associated with heightened regulated supervision (Davis column 2 lines 1-11).

*In reference to claims 2 and 9* wherein the single removable user unit is configured as a movable processing support uniquely assigned to the user (column 21 lines 11-14).

*In reference to claims 3 and 10,* wherein the single removable user unit configured as a smart card (column 21 lines 11-14).

*In reference to claims 6 and 13* wherein the enabling algorithm is incorporated into a stream of private data within said data streams (Davis column 7 lines 34-50).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the servers of Wasilewski to create the upgrade or modify cryptographic algorithm by an authorized entity as in Davis. One of ordinary skill in the art would have been motivated to do this because it may be possible to ease export restrictions and allow regional licenses for such modifiable cryptographic devices which would greatly reduce the costs associated with heightened regulated supervision (Davis column 2 lines 1-11).

*In reference to claims 5 and 12,* Wasilewski teaches of a system for conditional access where the service provider sends data streams in MPEG format, column 18, lines 32-35. The receiver extracts the EMM message from the data stream, column 5 lines 9-13, where it stores the information from the EMM, therefore must extract the information. It uses a control word that includes authorization information from the EMM, therefore it interprets the identification code contained in the EMM message, column 4 lines 52-58. Wasilewski teaches of an algorithm that generates the control word, which is used to decrypt the information, if the subscriber is entitled to watch the program, thus an enabling algorithm that is on the basis of the

Art Unit: 2135

authentication information (identification code). Wasilewski teaches a smart card and therefore a removable algorithm

2. **Claims 7 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Davis as applied to claims 3 and 13 above, and further in view of Spies (6, 055, 314).

Wasilewski and Davis do not expressly teach the processor transmitting information about the delivery of the service itself.

The system described by Spies can be activated by the user unit to transmit information about the confirmation of the purchase request, thus about the delivery of the service.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send information about the purchase as in Spies in the system of Wasilewski. One of ordinary skill in the art would have been motivated to do this because it would enable the system to carry out error checking and correct information that was not received correctly.

3. **Claims 4 and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Davis as applied to claims 1 and 8 above, and further in view of Jones et al (5, 623, 637).

Wasilewski and Davis do not expressly disclose a system with a trusted middleware function in the reception means and a trusted middleware function in the dynamic part.

Jones discloses an embodiment of a system where trusted software carries out an authentication algorithm on the IC card (smart card) as well as on the host, column 8 line 13-34.

Art Unit: 2135

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have a trusted middleware function in the static part (the host in the Jones system) and have a middleware in that dynamic part (the smart card). One of ordinary skill in the art would have been motivated to do this because the removable card allows data stored on the card to be made immediately available to the connected host computer, Jones column 2 lines 23-29.

4. **Claim 15** is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Davis as applied to claim 8 above, and further in view of Kaplan et al (6,141,339).

Wasilewski and Davis do not teach the use of Java cards.

Kaplan teaches of Java cards used to receive applets from service nodes, column 5 lines 59-61. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Java cards for the user unit. One of ordinary skill in the art would have been motivated to do this because Java applets provide the intelligence to support features, Kaplan column 5 lines 61-65.

### *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK  
Friday, May 25, 2007

## **DETAILED ACTION**

### ***Continued Examination Under 37 CFR 1.114***

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/20/07 has been entered.

### ***Response to Arguments***

Applicant's arguments filed 03/20/07 have been fully considered. The newly cited reference, Davis, is used to overcome the deficiencies of Wasilewski that are created by the newly added limitation.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. **Claims 1-3, 5-6, 8-10, and 12-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski et al (6,157,719) and further in view of Davis (6,058,478).

*In reference to claims 1 and 8,* Wasilewski discloses a method for the controlled delivery of digital services to a user, wherein said services are identified by respective stream of encoded

digital data emitted by said plurality providers (column 4 lines 20-23) and the user is provided with a receiver to receive said digital data streams from said plurality providers (Fig. 1), the receiver being selectively enabled to make use of determined services of a given provider (column 4 lines 41-50). The system includes a single removable user unit to be associated to said receiver for enabling the use of respective determined services of the provider (Fig. 12 in combination with column 21. lines 15-27). An identifying code is incorporated into the digital data stream for the user to enable to receive said determined services (column 4 line 64 to column 5 line 13). The single removable user unit is associated to a processing function capable of security functions by exploiting said identifying code to enable the receiver of the user to make use of said determined services (column 5 lines 23-27).

Wasilewski does not expressly disclose incorporating into the digital data streams respective enabling algorithms to be selectively loaded into the smart card of Wasilewski.

Davis discloses a cryptographic device being remotely modified only by proper authorization (abstract). Davis further discloses selectively loading said enabling algorithm into the user unit of each of the selective users (column 8 lines 15-20) based on the respective identifying codes, upgrade signature (column 9 lines 30-51). The enabling algorithm is generated by the provider and specific to the provider (column 9 lines 1-30).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the servers of Wasilewski to create the upgrade or modify cryptographic algorithm by an authorized entity as in Davis. One of ordinary skill in the art would have been motivated to do this because it may be possible to ease export restrictions and allow regional

licenses for such modifiable cryptographic devices which would greatly reduce the costs associated with heightened regulated supervision (Davis column 2 lines 1-11).

*In reference to claims 2 and 9* wherein the single removable user unit is configured as a movable processing support uniquely assigned to the user (column 21 lines 11-14).

*In reference to claims 3 and 10,* wherein the single removable user unit configured as a smart card (column 21 lines 11-14).

*In reference to claims 6 and 13* wherein the enabling algorithm is incorporated into a stream of private data within said data streams (Davis column 7 lines 34-50).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the servers of Wasilewski to create the upgrade or modify cryptographic algorithm by an authorized entity as in Davis. One of ordinary skill in the art would have been motivated to do this because it may be possible to ease export restrictions and allow regional licenses for such modifiable cryptographic devices which would greatly reduce the costs associated with heightened regulated supervision (Davis column 2 lines 1-11).

*In reference to claims 5 and 12,* Wasilewski teaches of a system for conditional access where the service provider sends data streams in MPEG format, column 18, lines 32-35. The receiver extracts the EMM message from the data stream, column 5 lines 9-13, where it stores the information from the EMM, therefore must extract the information. It uses a control word that includes authorization information from the EMM, therefore it interprets the identification code contained in the EMM message, column 4 lines 52-58. Waslewski teaches of an algorithm that generates the control word, which is used to decrypt the information, if the subscriber is entitled to watch the program, thus an enabling algorithm that is on the basis of the

Art Unit: 2135

authentication information (identification code). Wasilewski teaches a smart card and therefore a removable algorithm

2. **Claims 7 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Davis as applied to claims 3 and 13 above, and further in view of Spies (6, 055, 314).

Wasilewski and Davis do not expressly teach the processor transmitting information about the delivery of the service itself.

The system described by Spies can be activated by the user unit to transmit information about the confirmation of the purchase request, thus about the delivery of the service.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to send information about the purchase as in Spies in the system of Wasilewski. One of ordinary skill in the art would have been motivated to do this because it would enable the system to carry out error checking and correct information that was not received correctly.

3. **Claims 4 and 11** are rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Davis as applied to claims 1 and 8 above, and further in view of Jones et al (5, 623, 637).

Wasilewski and Davis do not expressly disclose a system with a trusted middleware function in the reception means and a trusted middleware function in the dynamic part.

Jones discloses an embodiment of a system where trusted software carries out an authentication algorithm on the IC card (smart card) as well as on the host, column 8 line 13-34.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to have a trusted middleware function in the static part (the host in the Jones system) and have a middleware in that dynamic part (the smart card). One of ordinary skill in the art would have been motivated to do this because the removable card allows data stored on the card to be made immediately available to the connected host computer, Jones column 2 lines 23-29.

4. **Claim 15** is rejected under 35 U.S.C. 103(a) as being unpatentable over Wasilewski and Davis as applied to claim 8 above, and further in view of Kaplan et al (6,141,339).

Wasilewski and Davis do not teach the use of Java cards.

Kaplan teaches of Java cards used to receive applets from service nodes, column 5 lines 59-61. At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use Java cards for the user unit. One of ordinary skill in the art would have been motivated to do this because Java applets provide the intelligence to support features, Kaplan column 5 lines 61-65.

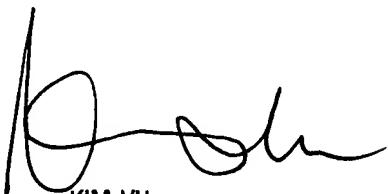
### *Conclusion*

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK  
Friday, May 25, 2007



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100